

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Frenkel, et al.
Serial No.: 10/581,437
For: Method and Apparatus for Combining Traffic Analysis and Monitoring
Center in Lawful Interception
Filed: June 2, 2006
Examiner: SHIN-HON CHEN
Art Unit: 2431

Attorney Docket Number 0004813USU/4269

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

In response to the Office Action dated November 24, 2009, Appellants file herewith a Notice of Appeal and request review of the present application before the filing of an appeal brief.

Status of the Claims

Pending claims 1-24 are finally rejected and are the subject of this request for review.

Claims 1-24 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Pub. No. 20050127171 by Ahuja.

1. Clear Error for Review: Ahuja fails to disclose receiving intercepted (captured) communication

"Lawful interception" of communications as generally referred to relates to obtaining communications network data pursuant to lawful authority for the purpose of analysis or evidence. Lawful interception thus does not prevent the intercepted communication from reaching its destination.

Thus, in the current application, which relates to lawful interception, the intercepting party has interest in the communication taking place and in obtaining the communication, for the purpose of collecting information. As further detailed below, the communication is intercepted for enriching the data available to the law enforcement agency.

Ahuja, on the other hand, is aimed at the contrary, which is to stop the interaction and halt the delivery of documents to a destination outside of the organization. Ahuja has no interest in the captured interaction, since its content is anyway available to the organization.

Accordingly, Ahuja does not teach receiving lawfully intercepted communication of a target.

2. Clear Error for Review: Ahuja fails to disclose receiving the communication itself, and relates only to attached documents.

The present disclosure is aimed at enriching the knowledge obtained from the intercepted communications performed by a target, for which a warrant has been issued. Ahuja is aimed at stopping only documents from going out of the organization network. Ahuja relates only to documents implemented as files, see for example ¶0045 of Ahuja:

"alert the user if all or part of the content in the registered document is leaving the network. Thus, one embodiment of the present invention aims to prevent un-authorized documents of various formats (e.g., Microsoft

Word, Excel, PowerPoint, source code of any kind, text) from leaving an enterprise."

Moreover, in Ahuja documents have to be registered with the system (i.e. become registered documents) to enable their interception. Therefore, Ahuja requires a preliminary registration stage for a document, and cannot be used for capturing communications of a target, such as phone calls.

The present application, however, relates to receiving the mere captured communication, in which the target participates (otherwise the warrant is not applicable), such as phone conversations, chat sessions, web browsing history, VoIP communications, e-mail messages (and not only documents attached to such messages), faxes, video recordings or other activity or communications. See ¶10018 of the present application. Appellants submit, therefore, that Ahuja does not teach receiving data or content of a communication in which a target participates, as required by the independent claims.

3. Clear Error for Review: Ahuja fails to disclose communication intercepted in accordance with a warrant.

The present application relates to capturing interactions of a target by a law enforcement agency, in accordance with a warrant. A warrant is external to an organization. Further, the organization may not be the source of the information. For example, interception can be done at an ISP, phone company, or the like.

Ahuja, however, describes a system which is totally internal to an organization, that is implemented within the organization's LAN, and that is aimed at stopping documents from exiting the organization. Naturally, no warrant is required for protecting the organization's own information, and no mechanism is required for applying a warrant in order to intercept documents. Appellants submit, therefore, that Ahuja does not teach intercepting a communication of a target, in accordance with a warrant, as required by the independent claims.

4. Clear Error for Review: Ahuja fails to disclose receiving a stored record and integrating the intercepted interaction with the stored record.

Claim 1 requires receiving a stored record and analyzing the stored record *with* the captured interaction, in order to enrich the knowledge of the law enforcement organization. This integration and data enriching is demonstrated for example in FIGS. 2A-2C and ¶¶0019-0021 of the present application. Thus, the present application relates to integrating at least two pieces of data. Ahuja, however, uses the stored records only for determining whether a particular document is registered and should therefore be intercepted. Thus, Ahuja does not analyze, integrate, or otherwise use the records together with the documents being intercepted. Further, Ahuja cannot use such information, since the records in Ahuja contain only tags of the documents and not substantial data relevant to the contents of the documents. See for example Ahuja at ¶¶0037 and Table 1. Appellants submit, accordingly, that Ahuja does not disclose integrating the at least one stored record in association with the intercepted communication, as required by the independent claims.

5. Clear Error for Review: Ahuja fails to disclose analyzing the intercepted interaction.

Claim 1 requires analyzing the stored record with the captured interaction, in order to enrich the knowledge of the law enforcement organization. The analysis refers, for example, to traffic analysis and content analysis, as detailed for example at ¶¶0025 of the Specification.

Ahuja, however, checks only the matching between the document and some criteria, does not analyze the captured information, and uses the stored records only for matching whether a particular document is registered and should therefore be intercepted. Therefore, the operation in Ahuja relates only to the technical characteristics of the document and not to its actual data or content as required by the independent claims.

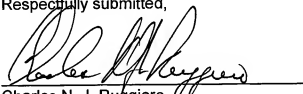
Thus, Appellants submit that Ahuja does not teach analyzing the information, but only stopping a document from leaving the organization boundaries.

In view of the above, it is respectfully submitted that the final rejection is clearly erroneous and, as such, the present application is in condition for allowance.

Reconsideration and withdrawal of the rejection of the claims and passage of the claims to allowance are respectfully requested.

Respectfully submitted,

February 24, 2010
Date


Charles N. J. Ruggiero
Reg. No. 28,468
Attorney for the Applicants
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th Floor
Stamford, CT 06901-2682
Tel: 203-327-4500
Fax: 203-327-6401